University of Plymouth

PEARL **https://pearl.plymouth.ac.uk**

Faculty of Science and Engineering School of Engineering, Computing and Mathematics

2016-12

Activity Recognition using wearable computing

Al-Naffakh, N

http://hdl.handle.net/10026.1/10426

10.1109/icitst.2016.7856695
2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)
IEEE

All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.

Activity Recognition using Wearable Computing

Neamah Al-Naffakh[1], Nathan Clarke[1,2], Paul Dowland[1], Fudong Li[1]
[1]Centre for Security, Communications and Network Research, Plymouth University, Plymouth, United Kingdom
[2]Security Research Institute, Edith Cowan University, Perth, Western Australia
{Neamah.Al-naffakh, N.Clarke, P.Dowland, Fudong.Li}@plymouth.ac.uk

Abstract— **A secure, user-convenient approach to authenticate users on their mobile devices is required as current approaches (e.g., PIN or Password) suffer from security and usability issues. Transparent Authentication Systems (TAS) have been introduced to improve the level of security as well as offer continuous and unobtrusive authentication (i.e., user friendly) by using various behavioural biometric techniques. This paper presents the usefulness of using smartwatch motion sensors (i.e., accelerometer and gyroscope) to perform Activity Recognition for the use within a TAS. Whilst previous research in TAS has focused upon its application in computers and mobile devices, little attention is given to the use of wearable devices – which tend to be sensor-rich highly personal technologies. This paper presents a thorough analysis of the current state of the art in transparent and continuous authentication using acceleration and gyroscope sensors and a technology evaluation to determine the basis for such an approach. The best results are average Euclidean distance scores of 5.5 and 11.9 for users' intra acceleration and gyroscope signals respectively and 24.27 and 101.18 for users' inter acceleration and gyroscope activities accordingly. The findings demonstrate that the technology is sufficiently capable and the nature of the signals captured sufficiently discriminative to be useful in performing Activity Recognition.**

Keywords- activity recognition; mobile authentication; accelerometer; smartwatch authentication.

I. INTRODUCTION

Over 9.5 billion mobile devices, including smartphones and tablets, are currently utilized for various purposes (e.g., personal communication, online payment, and office work); also these devices have increased amount of access to sensitive information such as financial or health records [1]. The data that is stored in the mobile device is often considered more valuable than the cost of the device itself [2]. Therefore, securing information on these devices from unauthorized access in an effective and usable fashion is essential. However, current user authentication approaches (such as password and PIN) are considered as intrusive that hinders their usability and subsequently the security of the mobile device and its data [3, 4]. According to a survey, 72% of their participants disabled the PIN code on their smartphones [5]; thus critical information that is stored on the device could be misused if it is lost or stolen. The use of Transparent Authentication Systems (TAS) is proposed in order to remove the user inconvenience (as the user is mainly transparently authenticated) and to improve the overall security in a continuous fashion [6]. Nevertheless, one of the key challenges for using transparent authentication is the lack of appropriate biometric modalities. In addition, previous research in this domain also encounters a performance issue due to the reliability of behavioural biometrics (i.e., the performance can be influenced by external environmental factors (e.g., mood)) [7].

Wearable computing becomes more prevalent in the market and it is predicted that the trend will continue as the technology improves. A survey showed that more than 80% of smartwatch consumers said that healthy living and medical care access are major benefits of wearable technology [8]. Due to their fixed contact with individuals (i.e., either left or right wrist), it is envisaged that smartwatches (e.g., LG and Microsoft Band 2) have the ability to capture more accurate personal data (e.g., acceleration and heart rate) than smartphones do. Therefore, wearables could be used to enhance the mobile security in a more effective way. Most modern smartwatches contain Micro Electro Mechanical System (MEMS) sensors, which are based upon a single chip that offers both tri-axial gyroscope and accelerometer capabilities. Normally, gyroscopes (offering rotational velocities) and accelerometers (measuring non-gravitational accelerations) are used on their own for a biometric system [9]. It is envisaged that the system performance can be improved if both of them are used together.

To this end, this paper explores the use of wearable computing for transparent authentication and in particular aims to investigate the feasibility of a novel *Activity Recognition* biometric modality. The rest of the paper is structured as follows: Section II reviews the state of the art in transparent and continuous authentication that uses acceleration and gyroscope sensors. A comprehensive evaluation on wearable technology is provided in Section III. Sections IV and V present the data collection, feature extraction, preliminary results and the proposed approach. Section VI presents the conclusions and future research directions.

II. BACKGROUND LITERATURE

Given the nature of wearable computing and its associated sensors, gait recognition is the modality that has the closest link to smartwatch-based activity recognition. Based upon how information is collected, gait recognition can be categorized into three main approaches: machine vision, wearable sensor, and mobile sensor. For the machine vision based approach, the movement of the human body is captured by using a fixed video-camera from a distance (such as CCTV) and it is mainly used for the identification purpose. In comparison, the other two approaches focus upon capturing

the periodic motion of the legs by attaching physical recording sensors on the human body such as hip, waist, lower leg, and arm or by carrying a mobile on the go; they are mainly used to verify the identity of the carrier. It is these studies that this review will focus upon. A comprehensive analysis of the prior studies on gait authentication using wearable and mobile sensors is summarized in Table I.

Table I. Comprehensive Analysis on Gait Authentication using Wearable and Mobile Sensors (C: Cycle-based; S: Segment-based; SF: Statistical Features; CF: Coefficient Features; DTW: Dynamic Time Warping; k-NN: k-Nearest Neighbors; HMM: Hidden Markov Model; SVM: Support Vector Machine; EER: Equal Error Rate; CCR: Correct Classification Rate; SD: Same Day; CD: Cross Days)

Study	Approach	Features Type	Classification methods	Accuracy %	Users	Duration (Seconds)
[10]	C	SF	Signal correlation	7 (EER)	36	30/CD
[11]	C	SF	Absolute distance	5 & 9 (EER)	21	60/SD
[12]	C	SF	DTW	6.7 (EER)	35	300/CD
[13]	C	SF	Euclidean distance	13 (EER)	99	60/SD
[14]	S	CF	Euclidean distance	10 (EER)	30	40/SD
[15]	C	SF	k-NN	95 (CCR)	7	90/SD
[16]	C	SF	Manhattan distance	5.7 (EER)	60	180/CD
[17]	C	SF	DTW	0.072 (EER)	32	600/SD
[18]	C	SF	k-NN	100 (CCR)	10	30/SD
[19]	C	SF	DTW	20.1 (EER)	51	120/CD
[20]	S	SF	J48 decision trees & Neural Network	100 (CCR)	5	300-600/SD
[21]	S	SF & CF	SVM	6.1 (EER)	48	120/CD
[22]	S	CF	SVM & HMM	10 &12.63 (EER)	36	1200/CD
[23]	C	SF	Manhattan & DTW	21.7 & 28 (EER)	48	1200/CD
[24]	C	SF	DTW & SVM	79 & 92.7 (CCR)	11	430/SD
[25]	S	SF & CF	SVM	10.1 (EER)	36	1200/CD
[26]	C	SF	DTW	29.4 (EER)	48	120/CD
[27]	S	CF	HMM	6.15 (EER)	48	1200/CD
[28]	C	SF	DTW	33.3 (EER)	51	60/CD
[29]	C	SF	SVM	91 (CCR)	14	420/SD
[30]	S	SF	Neural Network	98 (CCR)	8	80/SD
[31]	S	SF & CF	Random Forest, Multilayer Perceptron	98.3 & 98 (CCR)	59	300-600/SD
[32]	S	SF	Random Forest	93.3 (CCR)	17	2160/SD

The use of wearable sensors that are used to collect gait signals created a new domain for transparent and continuous user authentication on mobile devices. However, these studies are required to use specialized devices that are expensive for collecting the gait information; and the volume of their data per user is somewhat limited (i.e. 30 to 600 seconds) as illustrated in Table 1. Moreover, due to the complexity of the data collecting device, an additional cost would be required if they were utilised in a real-world system. Therefore, more recent studies attempted to utilize the smartphone built-in sensors for gathering the gait signal; as no extra cost is required. Also, this permits the authentication task to be performed in a transparent and continuous manner as the smartphone is carried in the user's pocket [19-30].

A large body of research on accelerometer-based activity recognition by using the same-day scenario (i.e. the training and testing data is collected on the same day) exist. In comparison, little work is considered by applying the cross-day evaluation scenario (which is a more realistic test as it shows the variability of the human gait behaviour over the time). Most research claim a system resilient to the cross-day problem either trains on data from trials that are also used to test (thus not making it a true cross-day system) or has a high error rate, preventing the system being used practically. The lack of realistic data underpins a significant barrier in applying gait recognition in practice.

To extract gait features from the captured signal, previous studies have focused upon two main approaches: cycle-based and segment-based. The former attempts to detect the periodic steps of the individuals by standardizing the number of steps as opposed to the amount of time represented in each instance (i.e. pace independent). The latter focuses on fixed-length blocks of data (without prior identification of the contained gait cycles). The literature shows that the performance varies significantly by using these two methods. The cycle extraction purportedly offers an exciting opportunity if a system is implemented effectively and trained in just a manner of steps; however, the error rate of using this approach is considered as high: the EER is ranging from 20.1% [19] to 33.3% [28] as demonstrated in the table 1. The high error rate is most likely caused by the result of the complicated and unclear nature of cycle extraction, as gait is only semi-periodic and the signals originating from smartphones are noisy due to a number of factors (e.g. the device not being securely fastened to the user, cheap sensors, and rounding errors). Furthermore, cycles are not guaranteed to be the same length and can vary widely in length depending on the pace of how a user walks; cycle extraction must be paired with a system that normalizes the length of each step, which adds another parameter to be configured and constantly refined. In contrast, the segmentation based method focuses on fixed-length blocks of gait data. While the segmentation based method is simple to implement, there is no guarantee on how many steps are completed within a given time window (there could be no full step at all). However, the performance of the segment based method appears to be more effective and stable, with studies reporting EERs between 6.1% and 10.1% [21, 25]. If the CCR were used, the performance of segment based method is even better: in the range of 93.3%-100% of the CCR [20, 32].

With respect to features, several studies in the literature have suggested that both statistical features (e.g., standard deviation, average, and N-bin histogram) and cepstral coefficient features (e.g., Mel Frequency Cepstral Coefficients (MFCCs) and Bark Frequency Cepstral Coefficients (BFCCs)) can be used to produce better performance [18, 20, 21, 22, 25, 27, 30, 31]. In addition, some studies only used the combination of MFCCs and BFCCs features alone and still

managed to produce a good level of results [21, 27]. The improvement on the performance of sensor based biometric systems can be attributed to more intricate feature vectors that utilize more complex features (e.g. MFCC and BFCC).

In terms of matching/classification, several classification methods (e.g., Absolute, Euclidean, and Neural Networks) can be used for training and testing phases. Many researchers prefer traditional approaches where a single template is generated and is later tested based upon the similarity between the template and the test data. By using this principle, various EERs between 5 and 33.3% were obtained from the following studies [10, 11, 12, 13, 14, 16, 17, 19, 23, 26, 28]. While this approach works well for physiological biometric methods (e.g., face or fingerprint), it is less effective for behavioural biometric techniques (e.g., body movement and keystroke dynamics). This is because the user's behaviour can change over time and be affected by other factors (e.g., mood and health). Therefore, it is more reasonable to collect user's multiple instances on multiple days and apply more complex algorithms (e.g., HMM and Neural Networks) upon them for generating the template and performing the classification process. Recent studies on mobile accelerometer-based gait authentication and smartwatch-based activity recognition demonstrate that by promising results are obtained by using advanced techniques (e.g., decision-tree based classifiers, and neural networks) [18, 20, 21, 22, 25, 27, 29, 30, 31].

Based upon the classification result, a decision on whether to accept or reject the output is made by the system. Accordingly to the literature, two standard schemas are used: majority or quorum voting. A better performance is normally obtained by using the quorum voting technical while the system is more resilient to error when the majority voting is applied. Under the quorum voting scheme, a small number of correct classification outputs are required to accept a user. While this will improve the user convenience (i.e., the user will be highly likely to accept the deployment of such system), it will result a high false acceptance rate (i.e., there is a high chance for the imposter to abuse the system). In contrast, more discriminative user behaviour is required when utilizing the majority voting technique; otherwise, a high false rejection rate will be produced by the system. It is understood that the system will provide a better security when using the majority voting method; at the same time, the system is more intrusive (i.e., less user friendly). As a result, it is important that a proper decision logic that can balance the system security and user convenience is applied for the gait authentication system.

The majority of previous studies collected the user's movement data by placing a smartphone in a fixed position (e.g., in the trouser pocket or on the hip). It is widely understood that smartphones suffer from several issues to produce a consistent and reliable data collection in real life; these include the problem of orientations (i.e., screen rotations) and off-body carry (e.g., when the device is carried in a handbag), making the data collection process less accurate or nearly impossible. In contrast, smartwatches provide a more consistent user's motion data collection as it is almost fixed to the user (i.e., it is worn on either left or right hand) regardless of their clothing choices. In addition, the smartwatch can provide a consistent orientation (i.e., it is worn in such a way that the text on screen is easily readable to the user). As a result, smartwatches offer the opportunity to collect the user's motion data in a more effective and reliable fashion than smartphones could. With the aim of exploring the possibility of using smartwatches to collect user's movement data, an evaluation of existing wearable technology is presented in the following section.

III. TECHNOLOGY EVALUATION

Despite a wide variety of manufacturers existing in the wearable market, the functionalities and available sensors within various smartwatches are similar. Developers can collect data from these devices and transmit it to a smartphone via Bluetooth, enabling the data to be further analysed. A comparison of several important features on the smartwatches (e.g., the embedded sensors, cost, and battery life) is presented in Table II.

Table II. Comprehensive Evaluation of Wearable Technology

Features	Microsoft Band 2	Samsung Gear	LG Urbane	Apple Watch
Sensors	Accelerometer (Accel) Gyroscope Compass Heart rate Ambient light GPS Skin temperature	Accel Gyroscope Compass ECG	Accel Gyroscope Compass PPG Barometer	Accel Gyroscope Heart rate Ambient light sensors Pulse oximeter
Smartphone compatibility	Android 4.3 and later , iOS 8.2 or newer, Windows 8.1 or later	Android 4.3 and later	Android 4.3 and later , iOS 8.2 or newer	iOS 8.2 and newer
Battery life	two days	one day	one day	two days
OS	Android	Tizen	Android	iOS
Price (in £)	150	190	160	340

As shown in Table II, all of the selected smartwatches offer the basic sensors: accelerometer and gyroscope. It is apparent that Microsoft Band 2 has more sensors (e.g., GPS and Skin temperature) compared to other smartwatches. These sensors offer the opportunity to capture various personal based biometric-based data which can be useful for a transparent and continuous based biometric system. Also, it can be connected to multiple mobile platforms (i.e., Android, iPhone and Windows Phone); therefore, there are no restrictions in order to collect data from a large pool of participants that have different types of smartphones. Unlike other smartwatch technologies, Microsoft Band 2 offer the opportunity to collect data in a continuous manner for at least 4 hours without recharging and thus offer the potential to collect a huge amount of real life data.

IV. PRELIMINARY ANALYSIS OF ACTIVITY RECOGNITION

With the aim of investigating the feasibility of using wearable computing for transparent user authentication, a preliminary study is conducted to capture and analyse the user's movement data. Details of the study, including data

collection, feature extraction and analysis are presented in the following subsections.

A. Data Collection and Transformation

In order to collect user's movement data, the Microsoft band 2 is utilized due to its wide range of built-in sensors. In addition to acceleration and gyroscope data (which are collected at a rate of 30-32 samples per second for the x, y and z axes). As soon as the data is collected by the smartwatch, it is sent to a smartphone residing in the user's pocket via Bluetooth. In total, 10 users participated for the data collection; each user is required to walk in two five-minute sessions on flat floor on two different days with their natural walking style. Also, users are free to choose which arm they wear the smartwatch on.

Once the data collection phase is completed, initial analysis on the data is carried out. Users' gait data (presented in the tri-axial raw format for both acceleration and gyroscope signals) are segmented into 10-second segments by using a sliding window approach with no overlapping. Examples of the acceleration and gyroscope data along the X, Y, and Z axes of two users are illustrated in Figures 1 and 2 respectively. Discriminating patterns can be clearly observed between the acceleration and gyroscope data of the selected two users across the X, Y and Z axes, preliminarily suggesting users have distinctive movements that would be used to transparently and continuously authenticate individuals.

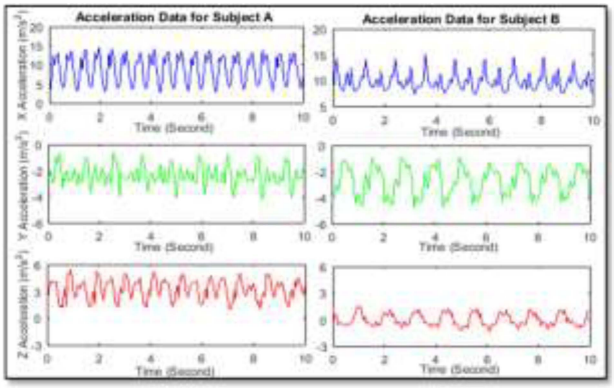

Fig 1: Acceleration Sample of Three Different Axes for Subject A and B

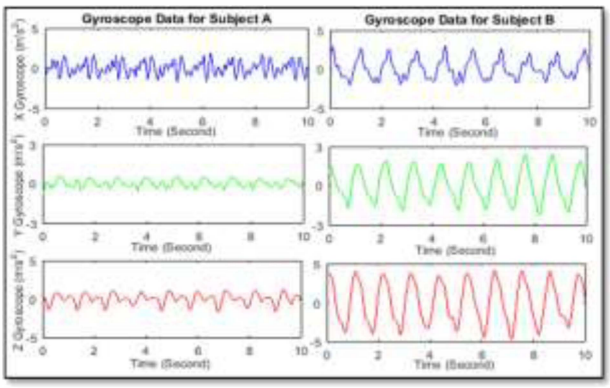

Figure 2. Gyroscope Sample of Three Different Axes for Subject A and B

Also, a feature extraction process is carried out on both the acceleration and gyroscope data segments of each user. In total 88 unique features are created. Details of these features (e.g., what they are and how they are calculated) are presented below; also the number of generated features for each type is specified in brackets.

- **Average (3):** the mean of the values in the segment (each axis)
- **Standard Deviation (3):** the Standard Deviation of the values in the segment **(**each axis)
- **Average Absolute Difference (3):** the average absolute distance of all values in the segment from the mean value over the number of data point in the segment (each axis).
- **Time Between Peaks (3):** during the user's walking, repetitive peaks are generated in the signal. Thus, the time between consecutive peaks was calculated and averaged (each axis).
- **Binned Distribution (30):** relative histogram distribution in linear spaced bins between the minimum and the maximum acceleration in the segment. Ten bins are used for each axis.
- **Average Resultant Acceleration (1):** for each value in the segment of x, y, and z axes, the square roots of the sum of the values of each axis squared over the segment size (i.e., 10 seconds) is calculated.
- **MFCC (39):** The first 13 Mel Frequency Cepstral Coefficients (each axis).
- **Variance (3):** The second-order moment of the data (each axis).
- **Covariance (3):** All pairwise covariances between axes.

B. Validating features extracted from the smartwatch

In order to validate the effectiveness of the 88 generated features for a promising authentication technique, the data set is divided to form both reference and testing templates for all users in two scenarios (i.e., Same-Day and Cross-Day). The average Euclidean distance between the reference template and testing templates is calculated; this distance value represents the similarity between the two templates: the smaller the value, the more similar between the reference and testing templates and vice versa. As a result, in order for this technique to work, a small distance value should be presented when the reference and testing templates are from the same user; while a large distance value should be expected when these templates are from different users – representing the intra and inter sample variances. Results on 10 users' movement data for the Same-Day and Cross-Day scenarios are presented in Tables 3 and 4 respectively.

As shown in Table III, for the Same-Day, the average Euclidean distance scores for acceleration templates of the same user are relative small: ranging from 5.5 (Subject 5) to 12.13 (Subject 3). Also, the distance scores for gyroscope templates of the same user are generally small in the range of 11.90 – 23.66, apart from two: Subject 4 (35.08) and Subject 6 (61.53). In comparison, average Euclidean distance scores for reference and testing templates of different users that are extracted on the same day are much larger: 10.69 (Subject 6)

to 24.27 (Subject 9) for acceleration and 31.85 (Subject 3) to 101.18 (Subject 5) for gyroscope. Table III shows that the results are completely based on the subject. The acceleration templates for all subjects, except subject 3, show that the user's arm movement is highly consistent and each subject has distinctive arm pattern characteristics. For gyroscope templates, some subjects (e.g., subjects 4 and 6) are difficult to recognize as their distance scores are very high while some are always recognized. It is also noted that the accelerometer is the better source sensor than gyroscope as the distance scores between the reference and test templates of the genuine user is small (i.e., low intra-variance), whereas the gyroscope data provides a significant distinguish between the genuine user and imposters (i.e., high inter-variance).

Table III. Results of Same-Day Scenario

Subject ID	Avg. Dist to Self		Avg. Dist to Others	
	Accel	Gyro	Accel	Gyro
1	6.70	18.18	12.58	47.35
2	8.58	20.86	15.77	94.49
3	12.13	13.27	19.50	31.85
4	8.68	35.08	19.08	56.77
5	5.50	23.66	15.40	101.18
6	6.80	61.53	10.69	85.44
7	6.86	12.43	15.99	87.70
8	8.65	11.90	23.68	49.13
9	9.30	15.35	24.27	34.61
10	9.45	19.79	24.21	51.07

Table IV. Results of Cross-Day Scenario

Subject ID	Avg. Dist to Self		Avg. Dist to Others	
	Accel	Gyro	Accel	Gyro
1	8.69	24	15.88	55.20
2	11.23	21.34	17.55	89.24
3	13.57	23.84	21.30	44.09
4	11.50	51.51	18.07	69.89
5	7.10	42.86	20.40	178.69
6	7.63	78.23	14.64	92.10
7	6.54	14.18	16.47	155.49
8	11.18	16.83	22.44	69.33
9	11.55	28.75	22.51	47.63
10	12.78	19.80	32.19	54.07

A more realistic test for a behavioural based-biometric comes when the cross-day scenario is applied to show the influence of the variation of human movement over time. Therefore, the cross-day scenario is also evaluated and the results shown in Table IV. While the distance scores under this more realistic evaluation scenario for acceleration and gyroscope templates of the genuine user is increased, they are actually still viable to be used for discriminating users: ranging from 6.54 (Subject 7) to 13.57 (Subject 3) for acceleration and from 14.18 to 28.75 for gyroscope (apart from two: subject 4 (51.51) and subject 6 (78.23)). In comparison, the resulting distance scores for reference and probe templates of imposters are generally quite high: 14.64 (Subject 6) to 32.19 (Subject 10) for acceleration and 44.09 (Subject 3) to 178.69 (Subject 5) for gyroscope, which is an indication that imposters are more likely to be rejected by the system. The results also show the necessity of using a sensor fusion approach (i.e., combining the smartwatch sensors data) in order to have a balance between security and usability (i.e., low false acceptance rate and low false rejection rate). The former shows the percentage in which the system incorrectly accepts an imposter as the legitimate user while the latter displays the percentage in which the authorized user is wrongly rejected by the system.

V. Proposed Architecture to Support Smartwatch-based Activity Recognition

A high-level architecture of the proposed system is presented in Figure 3. The prior art has established that managing the complex and varying signals of real-life use is a significant barrier. In order to overcome this, a context aware approach will be used in order to predict the user's activity at a specific point of time. This can be achieved by obtaining information from other smartwatch sensors (e.g., GPS) and using the information to create a multi-classifier approach that is trained to specific activities. This should result in reducing the variability in the feature set and provide better classification performance.

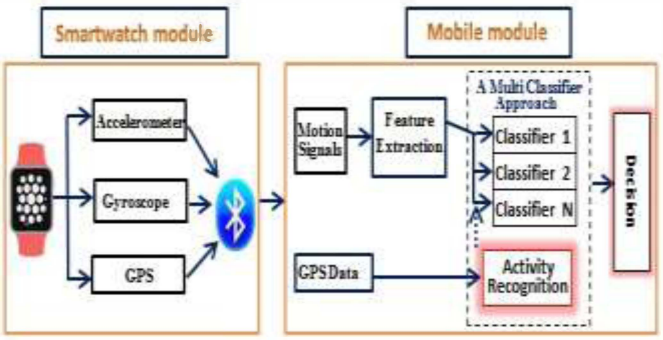

Figure3. The Proposed Architecture for the Motion-based Activity Recognition

Unlike most of the prior studies that utilized information from a single sensor only (i.e., accelerometer or gyroscope), the proposed system aims to collect the movement data of both sensors as well as GPS information. It is possible that the fusion of acceleration and gyroscope data would offer a greater level of accuracy than either sensor alone. Thereafter, feature selection needs to be sophisticated enough before the classification phase takes place. This can be achieved by selecting the features that are more resistant to changes of the user's behaviour. Finally, a set of classification methods will be evaluated to create a model for each individual activity.

VI. Conclusion and Future Work

In the experimental study, the raw movement data is collected from 10 subjects on two different days within a controlled environment (i.e., walking on flat floor only and each subject is asked to walk using their natural pace). Based on the results presented, this paper suggests that the user's movement data could be sufficient to be used for smartwatch based activity recognition but a thorough evaluation is required. It is expected that the performance from the cross-day scenario would not be as good as the result from the same-day scenario. Therefore, more experimental work should be carried out to investigate the impact of the selected features;

and the outcome will be used to improve the performance on the realistic situation (i.e., cross-day scenario).

Future work will include a scientifically valid experiment that involves collecting data from a large number of users over multiple days. Unlike most existing motion-based authentication studies implemented within a controlled environment (i.e., all participants were asked to perform specific activities in an indoor environment), a methodology will be developed to collect real life data (i.e., users do not need to perform certain activities, but to wear the smartwatch) to make sure that data can be used for real practical system. Moreover, each user will be asked to undertake multiple activities (e.g., different walking paces and typing on smartphone touch screen). As the nature of the real life signals is likely to be noisy, data from other smartwatch sensors (e.g. GPS) will be used in order to develop a context-aware approach (which will be useful to predict the user's activity).

ACKNOWLEDGMENT

The authors would like to thank the test subjects who participated in this study. I would also like to express my sincere gratitude to the University of Kufa for their financial support of this research.

REFERENCES

[1] M. Devices, M. E. Users, A. Pacific, and T. R. Group, "Mobile Statistics Report , 2015-2019," vol. 44, no. 0, pp. 0–2, 2015.

[2] Lifestylegroup, "Data stored on a phone more precious than the phone itself," 2011. [Online]. Available: http://www.lifestylegroup.co.uk/content/Data-stored-on-a-phone-more-precious-than-the-phone-itself.html. [Accessed: 27-Feb-2016].

[3] N. L. Clarke and S. M. Furnell, "Advanced user authentication for mobile devices," *Comput. Secur.*, vol. 26, no. 2, pp. 109–119, 2007.

[4] C. G. Hocking, S. M. Furnell, N. L. Clarke, and P. L. Reynolds, "Co-operative user identity verification using an Authentication Aura," *Comput. Secur.*, vol. 39, no. PART B, pp. 486–502, 2013.

[5] M. Hamblen, "Mobile phone security no-brainer: Use a device passcode,"2013. [Online]. Available: http://www.computerworld.com/article/2497183/mobile-security/mobile-phone-security-no-brainer--use-a-device-passcode.html.[Accessed:01-Mar-2016].

[6] N. Clarke, Transparent user authentication: biometrics, RFID and behavioural profiling. Springer London, 2011

[7] H. Saevanee, N. L. Clarke, and S. M. Furnell, "Multi-modal Behavioural Biometric Authentication for Mobile Devices," in *IFIP Advances in Information and Communication Technology*, vol. 376 AICT, 2012, pp. 465–474.

[8] PcW, "The Wearable Future" *Camden New Ser.*, vol. 39, p. iii, Jul. 2015.

[9] H. Lau and K. Tong, "The reliability of using accelerometer and gyroscope for gait event identification on persons with dropped foot," *Gait Posture*, vol. 27, no. 2, pp. 248–257, 2008.

[10] J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S. Makela, and H. Ailisto, "Identifying Users of Portable Devices from Gait Pattern with Accelerometers," in *Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.*, 2005, vol. 2, pp. 973–976.

[11] D. Gafurov, K. Helkala, and T. Søndrol, "Biometric gait authentication using accelerometer sensor," *J. Comput.*, vol. 1, no. 7, pp. 51–59, Nov. 2006.

[12] L. Rong, D. Zhiguo, Z. Jianzhong, and L. Ming, "Identification of Individual Walking Patterns Using Gait Acceleration," in *2007 1st International Conference on Bioinformatics and Biomedical Engineering*, 2007, pp. 543–546.

[13] D. Gafurov, E. Snekkenes, and P. Bours, "Spoof Attacks on Gait Authentication System," *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 3, pp. 491–502, Sep. 2007.

[14] D. Gafurov and E. Snekkkenes, "Arm Swing as a Weak Biometric for Unobtrusive User Authentication," in *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2008, pp. 1080–1087

[15] M. Nowlan, "Human Identification via Gait Recognition Using Accelerometer Gyro Forces Michael Fitzgerald Nowlan CPSC-536-Networked Embedded Systems and Sensor Networks Professor Savvides Fall 2009 2 . Related Work and Human Gait," p. 8, 2009.

[16] M. O. Derawi, P. Bours, and K. Holien, "Improved Cycle Detection for Accelerometer Based Gait Authentication," in *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2010, pp. 312–317.

[17] N. T. Trung, Y. Makihara, H. Nagahara, R. Sagawa, Y. Mukaigawa, and Y. Yagi, "Phase registration in a gallery improving gait authentication," in *2011 International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–7.

[18] Sangil Choi, Ik-Hyun Youn, R. LeMay, S. Burns, and Jong-Hoon Youn, "Biometric gait recognition based on wireless acceleration sensor using k-nearest neighbor classification," in *2014 International Conference on Computing, Networking and Communications (ICNC)*, 2014, pp. 1091–1095.

[19] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition," in *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2010, pp. 306–311.

[20] J. R. Kwapisz, G. M. Weiss, and S. a Moore, "Cell phone-based biometric identification," in *2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2010, pp. 1–7.

[21] C. Nickel, H. Brandt, and C. Busch, "Classification of Acceleration Data for Biometric Gait Recognition on Mobile Devices," 2011.

[22] C. Nickel, H. Brandt, and C. Busch, "Benchmarking the performance of SVMs and HMMs for accelerometer-based biometric gait recognition," in *2011 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, 2011, pp. 281–286.

[23] C. Nickel, M. O. Derawi, P. Bours, and C. Busch, "Scenario test of accelerometer-based biometric gait recognition," in *2011 Third International Workshop on Security and Communication Networks (IWSCN)*, 2011, pp. 15–21.

[24] H. M. Thang, V. Q. Viet, N. Dinh Thuc, and D. Choi, "Gait identification using accelerometer on mobile phone," *2012 Int. Conf. Control. Autom. Inf. Sci.*, pp. 344–348, 2012.

[25] M. R. Hestbek, C. Nickel, and C. Busch, "Biometric gait recognition for mobile devices using wavelet transform and support vector machines," pp. 205 – 210, 2012.

[26] M. Muaaz and C. Nickel, "Influence of different walking speeds and surfaces on accelerometer-based biometric gait recognition," in *2012 35th International Conference on Telecommunications and Signal Processing (TSP)*, 2012, pp. 508–512.

[27] C. Nickel and C. Busch, "Classifying accelerometer data via Hidden Markov Models to authenticate people by the way they walk," in *2011 Carnahan Conference on Security Technology*, 2011, vol. 28, no. 10, pp. 1–6.

[28] M. Muaaz and R. Mayrhofer, "An Analysis of Different Approaches to Gait Recognition Using Cell Phone Based Accelerometers," in *Proceedings of International Conference on Advances in Mobile Computing & Multimedia - MoMM '13*, 2013, pp. 293–300.

[29] T. Hoang, T. Nguyen, C. Luong, S. Do, and D. Choi, "Adaptive Cross-Device Gait Recognition Using a Mobile Accelerometer," *J. Inf. Process. Syst.*, vol. 9, no. 2, pp. 333–348, Jun. 2013.

[30] Y. Watanabe, "Toward Application of Immunity-based Model to Gait Recognition Using Smart Phone Sensors: A Study of Various Walking States," *Procedia Comput. Sci.*, vol. 60, pp. 1856–1864, 2015.

[31] A. H. Johnston and G. M. Weiss, "Smartwatch-based biometric gait recognition," in *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2015, pp. 1–6.

[32] G. M. Weiss, J. L. Timko, C. M. Gallagher, K. Yoneda, and A. J. Schreiber, "Smartwatch-based activity recognition: A machine learning approach," in *2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*, 2016, pp. 426–429.